Resources to support practices with DSP Submissions and GDPR compliance 2019-2020

Note- changes or additions to this resource since the last version have been marked on this document in blue

1. **Resources to Support practices with DSP Submissions and GDPR compliance (this document)**

   This a brief overview of the resources available to assist you in compliance to GDPR and the DSP toolkit. Please feel free to amend any of the resources as you see fit. The "Toolkit for the Toolkit" is the key document and we advise you read this first, as all subsequent documents are referenced within it. Each document number within this document is referenced within the appropriate document title. If you have any queries please contact the CCG IG team via Leedsccg.dpo@nhs.net

   There are a number of new documents included in this this year's toolkit to reflect some of the changes

2. **"Toolkit for the Toolkit"**

   This is a list showing each assertion (question) within the new DSP that requires an answer- some are mandatory and some are non-mandatory. We have tried to provide guidance for all assertions, whether mandatory or not. Many of the guidance notes refer to documents explained within this list.

   We have indicated where this requirement has changed from last year

3. **Information Asset Register and Data Flow Map template ("Article 30 Register")**

   This is a spreadsheet workbook that has two purposes- one sheet shows a list of possible Information Assets (the Information Asset Register) and the other lists data flows. As well as being part of the DSP you are also required to have this in place as part of your general GDPR compliance under Article 30. We have included as many possible assets and data flows as possible, and put in the legal basis you have for having this information. Any that do not apply to your practice you can remove- of there any any processes not included you can add them. We have also built in a few extra columns to show if the suppliers are GDPR compliant, whether the system support individual sign on etc. as these questions also feature in the DSP

4. **Policies**

There are a number of policies that you should have in place for DSP/GDPR compliance-if you do not already have them in place we have created sample policies you can use from the ones we created for the CCG- you will need to add in your own details etc.

a. Confidentiality and Data Protection Policy- addition of a new executive summary to clarify the position of the practice and some minor amendments
b. Data and Information Security Policy- addition of a new executive summary to clarify the position of the practice and some amendments to reflect the uncertainty around transfer of data outside the UK, post Brexit
c. Data Quality Policy- addition of a new executive summary to clarify the position of the practice and some minor amendments
d. Network Security Policy- reviewed and minor amendments made
e. FOI Policy (new)
f. Subject Access Request (SAR) Policy (new) which also provides advice on redaction and disclosure.
g. Smartcard Registration Authority Policy statement

5. Data Privacy by Design and Default

As part of your compliance you are expected to have built in privacy by design and default- the purpose of these documents is to assess any new data processing tasks.

We have developed a broad Data Privacy by Design and Default policy which outlines your organisation's commitment to DPDD

There are two forms included- one for data processing activities changes you instigate (e.g. changing a supplier) and one for changes imposed upon you (e.g. if another organisation changes the way it sends data to you etc.)

a. For practice proposed changes
b. For imposed changes

6. Privacy Notice

As part of your compliance you need to have a Privacy or Fair Processing notice in place (we have developed from original material developed from Lindsay Gollin, Business Manager, Allerton Medical Centre) updated to include all items required for GDPR compliance- you will need to amend this to your own needs by adding your details.

This has been amended slightly from the edition we published last year and a section has been added to reflect the role of PCNs. All changes have been marked via Tracked Changes.

7. Subject Access Request (SAR) form

You will require a SAR procedure for compliance- we have developed one which combines the SAR request with the fair processing data you should supply when releasing SARs under Article 15 of GDPR. This document has remained unchanged since last year.

This can be used in conjunction with the new SAR policy

8. GDPR Guidance for GP Staff

This is short guide to GDPR and how it impacts on the way the practices manages data.

9. IG Spot Check template

You are required to carry out “Spot checks” on IG and security- this template allows you to record your observations and recommendations

10. Retention schedule documents

All data you hold is subject to a retention schedule- this contains the accepted retention schedules for data. If you have data that does not match the criteria outlined, you can get assistance from: Leedsccg.DPOe@nhs.net

We have added two documents this year- one is taken from the Information Governance Alliance guidance and the other is a new document adapted from a CCG retention schedule we have developed and incorporates a Retention Schedule policy that relates to the retention schedule spreadsheet . You do not have to use these retention schedules, although they have been developed to ensure they are compliant with the appropriate statute and/or best practice.

11. “how we use your information” for GP staff

This is a short guide for staff about how the practice, as their employer, uses their data

12. Staff IG awareness survey

Although not mandatory this year, there are 17 questions which form the National Staff IG awareness survey.
Rather than 17 different assertions (as in last years submission), these have not been consolidated into one assertion (2.2.3)

13. Personal Data breach (ICO) log and disclosure log

All data breaches should be logged via Datix, however the spreadsheet is to log any and all incidents referred to the ICO. This can be used in conjunction with the Data Breach Guidance

This has been amended this year to also include a disclosure log on sheet 2

14. Example Risks

we have supplied you with a list of sample risks you may wish to consider- we have also undertaken a root cause analysis of all IG incidents reported via DATIX from GP practices over the period of one year and have included this as part of the updated guidance.

15. Data Breach Guidance

Documentation provided by NHS Digital regarding how to identify, evaluate and report Data Breaches

16. Patch schedules

This is a document detailing how updates are applied to your system- one has been provided for practices managed by Egton, the other for practices managed by LCC (or for practices which used to be managed under the old Embed contract).